PORTAL

USPTO

Search:　◉ The ACM Digital Library　○ The Guide

((application-specific) and (intrusion))

THE ACM DIGITAL LIBRARY

Feedback　Report a problem　Satisfaction survey

Terms used **application** **specific** and **intrusion**　　　　　　Found **3,409** of **169,866**

| Sort results by | relevance |
| Display results | expanded form |

◈ Save results to a Binder
⍰ Search Tips
☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200　　　Result page: **1**　2　3　4　5　6　7　8　9　10　　next
Best 200 shown　　　　　　　　　　　　　　　　　　　　Relevance scale ☐ ▨ ▩ ▨ ▩

1　Computer security: Service specific anomaly detection for network intrusion detection ▩
Christopher Krügel, Thomas Toth, Engin Kirda
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing**
Publisher: ACM Press

Full text available: 📄 pdf(719.17 KB)　　Additional Information: full citation, abstract, references, citings, index terms

The constant increase of attacks against networks and their resources (as recently shown by the CodeRed worm) causes a necessity to protect these valuable assets. Firewalls are now a common installation to repel intrusion attempts in the first place. Intrusion detection systems (IDS), which try to detect malicious activities instead of preventing them, offer additional protection when the first defense perimeter has been penetrated. ID systems attempt to pin down attacks by comparing collected d ...

Keywords: anomaly eetection, intrusion eetection, network security

2　Intrusion detection techniques for mobile wireless networks　　　　　　　　▩
Yongguang Zhang, Wenke Lee, Yi-An Huang
September 2003 **Wireless Networks**, Volume 9 Issue 5
Publisher: Kluwer Academic Publishers

Full text available: 📄 pdf(164.73 KB)　　Additional Information: full citation, abstract, references, citings, index terms

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. We need to search for new architecture and mechanisms to protect the wireless networks and mobile computing application. In this paper, we examine the vulnerabilities of wireless networks and argue that we must include intrusion detection in the securit ...

Keywords: anomaly detection, cooperative detection, intrusion detection, intrusion response, mobile ad-hoc networks

3　Securing information: Guarding the next Internet frontier: countering denial of ▩
information attacks
Mustaque Ahamad, Leo Mark, Wenke Lee, Edward Omicienski, Andre dos Santos, Ling Liu, Calton Pu
September 2002 **Proceedings of the 2002 workshop on New security paradigms**
Publisher: ACM Press

Full text available:　　　　　　　　Additional Information:

pdf(918.49 KB)   full citation, abstract, references, index terms

As applications enabled by the Internet become information rich, ensuring access to quality information in the presence of potentially malicious entities will be a major challenge. Denial of information (DoI) attacks attempt to degrade the quality of information by deliberately introducing noise that appears to be useful information. The mere availability of information is insufficient if the user must find a needle in a haystack of noise that is created by an adversary to hide critical informat ...

Keywords: countering information attacks, quality of information

4 Intrusion detection in wireless ad-hoc networks

Yongguang Zhang, Wenke Lee
August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking**
Publisher: ACM Press

Full text available: pdf(936.44 KB)   Additional Information: full citation, abstract, references, citings, index terms

As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. Ho ...

5 Software Engineering for Secure Systems (SESS) --- Building Trustworthy Applications: Using dynamic information flow analysis to detect attacks against applications

Wes Masri, Andy Podgurski
May 2005 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications SESS '05**, Volume 30 Issue 4
Publisher: ACM Press

Full text available: pdf(243.45 KB)   Additional Information: full citation, abstract, references, index terms

This paper presents a new approach to using dynamic information flow analysis to detect attacks against application software. The approach can be used to reveal and, under some conditions, to prevent attacks that violate a specified information flow policy or exhibit a known information flow signature. When used in conjunction with automatic cluster analysis, the approach can also reveal novel attacks that exhibit unusual patterns of information flows. A set of prototype tools implementing the a ...

Keywords: Computer security, dynamic information flow analysis, intrusion detection, observation-based testing, program dependences

6 Automated analysis: Control-flow integrity

Martín Abadi, Mihai Budiu, Úlfar Erlingsson, Jay Ligatti
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Full text available: pdf(218.60 KB)   Additional Information: full citation, abstract, references, index terms

Current software attacks often build on exploits that subvert machine-code execution. The enforcement of a basic safety property, Control-Flow Integrity (CFI), can prevent such attacks from arbitrarily controlling program behavior. CFI enforcement is simple, and its guarantees can be established formally even with respect to powerful adversaries. Moreover, CFI enforcement is practical: it is compatible with existing software and can be done efficiently using software rewriting in commodity syste ...

Keywords: binary rewriting, control-flow graph, inlined reference monitors, vulnerabilities

7 Intrusion detection: Anomaly detection of web-based attacks

Christopher Kruegel, Giovanni Vigna
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(252.97 KB)   Additional Information: full citation, abstract, references, citings, index terms

Web-based vulnerabilities represent a substantial portion of the security exposures of computer networks. In order to detect known web-based attacks, misuse detection systems are equipped with a large number of signatures. Unfortunately, it is difficult to keep up with the daily disclosure of web-related vulnerabilities, and, in addition, vulnerabilities may be introduced by installation-specific web-based applications. Therefore, misuse detection systems should be complemented with anomaly dete ...

Keywords: anomaly detection, network security, world-wide web

8 The taser intrusion recovery system

Ashvin Goel, Kenneth Po, Kamran Farhadi, Zheng Li, Eyal de Lara
October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5
Publisher: ACM Press

Full text available: pdf(346.32 KB)   Additional Information: full citation, abstract, references, index terms

Recovery from intrusions is typically a very time-consuming operation in current systems. At a time when the cost of human resources dominates the cost of computing resources, we argue that next generation systems should be built with automated intrusion recovery as a primary goal. In this paper, we describe the design of Taser, a system that helps in selectively recovering legitimate file-system data after an attack or local damage occurs. Taser reverts tainted, i.e. attack-dependent, file-syst ...

Keywords: file systems, intrusion analysis, intrusion recovery, snapshots

9 Incentive-based modeling and inference of attacker intent, objectives, and strategies

Peng Liu, Wanyu Zang, Meng Yu
February 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 1
Publisher: ACM Press

Full text available: pdf(963.16 KB)   Additional Information: full citation, abstract, references, index terms

Although the ability to model and infer attacker intent, objectives, and strategies (AIOS) may dramatically advance the literature of risk assessment, harm prediction, and predictive or proactive cyber defense, existing AIOS inference techniques are ad hoc and system or application specific. In this paper, we present a general incentive-based method to model AIOS and a game-theoretic approach to inferring AIOS. On one hand, we found that the concept of incentives can unify a large variety of att ...

Keywords: Attacker intent and strategy modeling, attack strategy inference, game theory

10 Efficient hierarchical self-scheduling for MPI applications executing in computational Grids

Cristina Boeres, Aline P. Nascimento, Vinod E. F. Rebello, Alexandre C. Sena

November 2005 **Proceedings of the 3rd international workshop on Middleware for grid computing MGC '05**

Publisher: ACM Press

Full text available: pdf(323.65 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

The execution of distributed applications on the grid is already a reality. As both the number of applications grow and grids scale, efficient utilization of the available but shared heterogeneous resources will be essential. The EasyGrid middleware is a hierarchically distributed Application Management System embedded into MPI applications to facilitate their efficient execution in computational grids. The overhead of employing a distinct AMS to make each application system aware does however b ...

Keywords: MPI applications, dynamic scheduling, grid computing, grid middleware, load balancing, process management

11 <u>The flight recorder: an architectural aid for system monitoring</u>

Michael M. Gorlick

December 1991 **ACM SIGPLAN Notices , Proceedings of the 1991 ACM/ONR workshop on Parallel and distributed debugging PADD '91**, Volume 26 Issue 12

Publisher: ACM Press

Full text available: pdf(944.95 KB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

12 <u>An intrusion tolerant architecture for dynamic content internet servers</u>

Ayda Saidane, Yves Deswarte, Vincent Nicomette

October 2003 **Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security**

Publisher: ACM Press

Full text available: pdf(551.49 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>

This paper describes a generic architecture for intrusion tolerant Internet servers. It aims to build systems that are able to survive attacks in the context of an open network such as the Internet. To do so, the design is based on fault tolerance techniques, in particular redundancy and diversification. These techniques give a system the additional resources to continue delivering the correct service to its legitimate clients even when active attacks are corrupting parts of the system compon ...

Keywords: adaptive redundancy, fault tolerance, intrusion tolerance

13 <u>Making operating systems more robust: Backtracking intrusions</u>

Samuel T. King, Peter M. Chen

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: pdf(185.10 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

Analyzing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of steps that occurred in an attack. The goal of BackTracker is to identify automatically potential sequences of steps that occurred in an intrusion. Starting with a single detection point (e.g., a suspicious file), BackTracker identifies files and processes that could have affected that detection point and displays chains of events i ...

Keywords: computer forensics, information flow, intrusion analysis

14 Backtracking intrusions

Samuel T. King, Peter M. Chen

February 2005 **ACM Transactions on Computer Systems (TOCS),** Volume 23 Issue 1

Publisher: ACM Press

Full text available: pdf(647.38 KB)   Additional Information: full citation, abstract, references, index terms

Analyzing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of steps that occurred in an attack. The goal of BackTracker is to identify automatically potential sequences of steps that occurred in an intrusion. Starting with a single detection point (e.g., a suspicious file), BackTracker identifies files and processes that could have affected that detection point and displays chains of events i ...

Keywords: Computer forensics, information flow, intrusion analysis

15 A Configurable Network Protocol for Cluster Based Communications using Modular Hardware Primitives on an Intelligent NIC

Ranjesh G. Jaganathan, Keith D. Underwood, Ron Sass

November 2003 **Proceedings of the 2003 ACM/IEEE conference on Supercomputing**

Publisher: IEEE Computer Society

Full text available: pdf(174.25 KB)   Additional Information: full citation, abstract

The high overhead of generic protocols like TCP/IP provides strong motivation for the development of a better protocol architecture for cluster-based parallel computers. Reconfigurable computing has a unique opportunity to contribute hardware level protocol acceleration while retaining the flexibility to adapt to changing needs. Specifically, applications on a cluster have various quality of service needs. In addition, these applications typically run for a long time relative to the reconfigurat ...

Keywords: Intelligent Network Interface Card, reconfigurable computing, networking protocols, cluster computing

16 Improving fine-grained irregular shared-memory benchmarks by data reordering

Y. Charlie Hu, Alan Cox, Willy Zwaenepoel

November 2000 **Proceedings of the 2000 ACM/IEEE conference on Supercomputing (CDROM)**

Publisher: IEEE Computer Society

Full text available: pdf(422.50 KB)   Additional Information: full citation, abstract, references, citings, index terms
Publisher Site

We demonstrate that data reordering can substantially improve the performance of fine-grained irregular shared-memory benchmarks, on both hardware and software shared-memory systems. In particular, we evaluate two distinct data reordering techniques that seek to co-locate in memory objects in close proximity in the physical system modeled by the computation. The effects of these techniques are increased spatial locality and reduced false sharing. We evaluate the effectiveness ...

17 Program visualization: the art of mapping programs to pictures

Gruia-Catalin Roman, Kenneth C. Cox

June 1992 **Proceedings of the 14th international conference on Software engineering**

Publisher: ACM Press

Full text available: pdf(1.10 MB)   Additional Information: full citation, references, citings, index terms

18 Sensor networks: Reputation-based framework for high integrity sensor networks

Saurabh Ganeriwal, Mani B. Srivastava

October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor**

networks
Publisher: ACM Press
Full text available: pdf(468.08 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

The traditional approach of providing network security has been to borrow tools from cryptography and authentication. However, we argue that the conventional view of security based on cryptography alone is not sufficient for the unique characteristics and novel misbehaviors encountered in sensor networks. Fundamental to this is the observation that cryptography cannot prevent malicious or non-malicious insertion of data from internal adversaries or faulty nodes.

We believe that in gen ...

Keywords: bayesian formulation, cryptography, framework, reputation, security, sensor networks, trust

19 <u>OS customization: An infrastructure for application-specific customization</u>
Arindam Banerji, David L. Cohn
September 1994 **Proceedings of the 6th workshop on ACM SIGOPS European workshop: Matching operating systems to application needs**
Publisher: ACM Press
Full text available: pdf(570.66 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>

As application requirements diverge, it is becoming increasingly clear that the *one size fits all* operating system design strategy is obsolete. Customizable system services would allow application-specific optimizations, and various customization strategies have been proposed. These vary widely and, depending on the required level of application-developer involvement, can be categorized as *parametric variation, interposition* or *synthesis* methods. We present a common architec ...

20 <u>A performance analysis model for distributed simulations</u>
David B. Cavitt, C. Michael Overstreet, Kurt J. Maly
November 1996 **Proceedings of the 28th conference on Winter simulation**
Publisher: ACM Press
Full text available: pdf(840.17 KB)   Additional Information: <u>full citation</u>, <u>references</u>, <u>citings</u>

Results 1 - 20 of 200   Result page: **1** <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> <u>10</u>   <u>next</u>

•

Freeform Search

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term:
`((application-specific) and (intrusion)).clm.`

Display: `10` Documents in **Display Format:** `-` **Starting with Number** `1`

Generate: ○ **Hit List** ◉ **Hit Count** ○ **Side by Side** ○ **Image**

Search | Clear | Interrupt

Search History

DATE: Monday, February 13, 2006   Printable Copy   Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L3	((application-specific) and (intrusion)).clm.	8	L3
L2	L1 and (SATYENDRA)	20	L2
L1	(yadav).inv.	617	L1

END OF SEARCH HISTORY